REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1, 6, 8, 9, 30, 32, 34, 54, 59, and 64 are pending in the application. Claims 1, 30, 32, and 34 are independent. The remaining claims depend, directly or indirectly, on claim 1, 30, 32, and 34.

Drawings

The Applicant respectfully requests that the Examiner indicate whether the drawings filed on September 8, 2000 are acceptable.

Claim Amendments

Claims 30, 32, and 34 have been amended to clarify how the digital identity data is bound to the microprocessor identity. Specifically, the following limitation has been added to each of the aforementioned independent claims: "wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity." Support for the aforementioned amendment may be found, for example, in Figure 7 of U.S. Provisional Patent Application Serial No. 60/179,989, which is incorporated by reference in the instant application, as well as on pages 8-9 of the instant application. No new matter has been added the aforementioned amendment.

Rejections under 35 U.S.C. §103

Claims 1, 6, 8, 9, 30, 32, 54, and 59 are rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,623,637 ("Jones") in view of U.S. Patent No. 5,237,610 ("Gammie") and U.S. Patent No. 5,774,544 ("Lee"). To the extent that this rejection applies to the amended claims, the rejection is respectfully traversed.

"To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." (*See* MPEP §2143). The Applicant respectfully asserts that the cited references do not teach all the claimed limitations. Further, the Applicant asserts that there is no motivation to combine the references to obtain the claimed invention.

With respect to teaching all the claimed limitations, the amended independent claims recite, in part, "wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity." The above limitation requires that: (i) the digital identity data be *encrypted*, (ii) the encryption is performed using an algorithm; and (iii) the algorithm uses the microprocessor identity.

The Examiner has asserted that Jones teaches encrypting the digital identity data. (*See* Office Action mailed December 13, 2005, p. 3). The Applicant respectfully disagrees. Specifically, the Examiner has asserted that "combining" a password with a random number is equivalent to "encrypting" digital identity data with the microprocessor identity. (*See* Office Action mailed December 13, 2005, p. 3). By asserting that "combining" is equivalent to "encrypting," the Examiner is completely misconstruing the broadest ordinary meaning of the term "encrypting." The term "encrypt" has a particular meaning in the art, which is laid out in the following excerpts of Jones:

> Encryption methods typically rely on "secret keys" known only to authorized users of the protected data. In the widely used Data Encryption Standard ("DES") developed and promulgated by the National Bureau of Standards, data is encyphered in 64-bit blocks using a single 56-bit key, as described in National Bureau of Standards' Federal Information Processing Standards Publication 46, "Data Encryption Standard," National Bureau of Standards (1977). *Encryption techniques using two keys, one for encypting the data and a different key for decryption, are called "public key" systems because the encryption key can be made public so that anyone can use the public key to encrypt sensitive data, but only a recipient with the secret key can decrypt it.* One widely used and highly effective public key algorithm known as the "RSA" system, named after the inventors Rivest, Shamer and Adelman, is described in Rivest et al. U.S. Pat. No. 4,405,829.
>
> The security of both single-key and public-key encryption systems depends on user's ability to keep the key or keys secret. Although both the DES and RSA encryption algorithms themselves can be depended upon to provide adequate security, neither system can safeguard data if the keys can be learned. The management of the keys themselves accordingly presents the most difficult component of good data security system. (Jones, col. 1, ll. 32-57).
>
> [...]
>
> To provide additional security, the data transferred over the 16-bit data bus between the data bus buffer 173 and the gate 178 is processed by the encryption-decryption unit 177 which preferrably emplements a symmetrical key algorithm, such as DES, based on a key value which stored in and fetched from the EEPROM 275 in the smartcard I.C. 250. *The unit 250 encrypts data from the data bus buffer 173 prior to storing the data in the common memory array 150, and decrypts the data back into its original form when it is retrieved from the common memory array 150. This additional encryption mechanism protects data*

> *stored in the common memory array even if that data is successfully read from the flash memory chips making up the array 150.* As discussed in more detail later, the secure key storage mechanism provided by the memory card may also be used to protect sensitive data being manipulated by mechanisms external to the memory card 100. (Jones, col. 6, ll. 5-21) [Emphasis added]

From the above excerpts, it is clear that when data is "encrypted" it is converted into a form that cannot be understood by others. Thus, in order for another to understand the encrypted data, the encrypted data must be decrypted (*i.e.,* returned to its original form). Said another way, once data is encrypted, it is unintelligible to unauthorized parties (*i.e.,* parties that are not supposed to be able to have access to the unencrypted data).

In view the above, "combining" cannot be construed to be equivalent to "encrypting," as "combining" does not operate to convert the data into a form that cannot be understood by those without the proper decryption key. Moreover, given the fact that Jones discusses the concept of encryption, if Jones had intended to "encrypt" the password and the random number, then it appears Jones would have taught that as opposed to merely reciting "combining."

In view of the above, Jones does not teach that which the Examiner asserts is taught. Further, Gammie does not teach that which Jones lacks. This is evidenced by the fact that Gammie is only relied upon to teach encrypting a key using a serial number and Lee is only relied upon to teach storing a microprocessor serial number in the NVRAM of a microprocessor. (*See* Office Action mailed December 13, 2005, p. 3).

Even assuming *arguendo* that Jones teaches encrypting using personal information, there is no motivation to combine Jones with Gammie. In fact, the portion of Gammie upon which the Examiner relies to show motivation to combine actually teaches away from combining Gammie with Jones. Specifically, the Examiner has asserted that one of ordinary skill in the art would be motivated to modify the system in Jones such that the random number (RN in Figure 1 of Jones) is replaced with a serial number of the device. (*See* Office Action mailed December 13, 2005, p. 3). In support of this assertion, the Examiner noted that "[o]ne skilled in the art would be motivated to do this because each serial number is unique to the individual device therefore the key will not be subject to compromise or recovery." (*See* Office Action mailed December 13, 2005, p. 3). If Jones is modified as suggested by the Examiner, the modified system would operate contrary to the Examiner's stated motivation to combine.

Specifically, the random number (RN in Figure 1 of Jones) is transmitted in clear text (*i.e.*, not encrypted) to the host computer. During this communication, the random number is subject to compromise and recovery. Said another way, the communication between the secure memory card and the host computer is subject to interception (*i.e.*, compromise). Further, if the communication is intercepted, the fact that is it not encrypted makes it subject to recovery.

Further, replacing the random number (*i.e.*, a number that changes with each use) in Jones with a serial number (*i.e.*, a number that is static) circumvents the challenge-response mechanism of Jones. In particular, Jones notes that:

> [p]referably, the validity of the stored access code is established by a challenge-and-response exchange of the type illustrated in FIG. 2, in which the remote computer 450 transmits a challenge in the form of a random number which is combined with the stored access code 425 to form a response which is returned to the remote computer 450 for verification. In this way, the access code 425 is not transmitted and interception of either the challenge or response values by an intruder monitoring the exchange will not provide the intruder with the access code. (Jones, col. 9, ll. 1-21).

Accordingly, if a serial number of the device, as opposed to a random number were used, then an intruder monitoring the exchange would, over time, be able to determine which portion of the challenge corresponds to the serial number because that portion of the challenge would always the be same. From this information, the intruder could extract the access code, thereby circumventing the challenge-response security measure. In view of the above, it does not appear that one of ordinary skill in the art would be motivated to modify the system of Jones with the teachings in Gammie.

Further, Lee does not provide that which Jones and Gammie lack as evidenced by the fact that Lee is only relied upon to teach storing a microprocessor serial number in the NVRAM of a microprocessor. (*See* Office Action mailed December 13, 2005, p. 3).

For the above reasons, the Examiner has not met their *prima facie* burden to assert that the claimed invention is obvious in view of Jones, Gammie, and Lee, whether considered separately or in combination. Accordingly, all pending independent claims are patentable over Jones, Gammie, and Lee. Dependent claims are patentable over Jones, Gammie, and Lee for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Claims 34 and 64 are rejected under 35 U.S.C. § 103 (a) as being obvious over Guthery in view of U.S. Patent No. 6,111,506 ("Yap").

At the outset, the Applicant asserts that the Examiner has failed to satisfy their burden under MPEP §707.07(f). Specifically, MPEP §707.07(f) requires that the Examiner "take note of the applicant's argument and answer it on substance." The Examiner did not follow this requirement. Rather, the Examiner merely reiterated the aforementioned rejection. In failing to address the arguments presented by the Applicant, the Examiner clearly failed to satisfy MPEP §707.07(f).

To the extent that the Examiner's rejection is proper, the Applicant respectfully traverses the rejection. At the outset, the Applicant notes that the Examiner likely intended this rejection to be based on Guthery, Yap, and Paolini, as evidenced by the content of the rejection on pages

6-8 of the Office Action mailed December 13, 2005. Accordingly, the reply to this rejection will address all three of the aforementioned references. In response to the aforementioned rejection, the Applicant reasserts all arguments made with respect to the corresponding rejection in the response mailed to the U.S. Patent Office on September 21, 2005. The relevant portions of previously presented arguments have been reproduced below for the Examiner's convenience.

> The Applicant respectfully asserts that neither Guthery nor Paolini, whether considered separately or in combination, teach or suggest the invention recited in the amended claims. Specifically, neither Guthery nor Paolini teach or suggest encrypting digital identity data associated with a user of the digital identity device using the microprocessor ID. In contrast, Guthery is directed to a system that merely includes a smart card having a microprocessor (52 in Figure 2) and information associated with the user of the smartcard (72 in Figure 2), without any mention of encrypting the user information with the microprocessor ID. In fact, Gurthry is completely silent with respect to a microprocessor including a microprocessor ID (*i.e.,* stored within the microprocessor).
>
> Similarly, Paolini fails to teach or suggest encrypting digital identity data associated with a user of the digital identity device using the microprocessor ID. Specifically, while Paolini does disclose a CPU ID (*See* Paolini, col. 3, ll. 2-19) and encrypting the software using the CPU ID (*See* Paolini, Fig. 2A), there is no teaching or suggestion of encrypting *digital identity data* (*i.e.,* data uniquely identifying a *user* of the digital identity device) with the CPU ID.
>
> [...]
>
> As discussed above, Guthery and Paolini fail to teach or suggest all the limitations of amended independent claim 1. Amended claim 34 includes at least

the same limitations with respect to the digital identity device as amended claim 1. Thus, Guthery and Paolini fail to teach or suggest all the limitations of amended independent claim 34. Further, Yap fails to teach that which Guthery and Paolini lack as evidenced by the fact that Yap is only relied upon to teach: (i) encrypting documents using a smart card and (ii) digital identity data (*See* Office Action mailed July 28, 2005, p. 9). In view of the above, claim 34 is patentable over Guthery, Paolini, and Yap. Accordingly, withdrawal of this rejection is respectfully requested.

In view of the previously presented arguments, claim 34 is patentable over Guthery, Yap, and Paolini. Dependent claim 64 is patentable over Guthery, Yap and, Paolini for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 05452/002002).

Dated: March 10, 2006

Respectfully submitted,

By________________________
T. Chyau Liang, Ph.D.
Registration No.: 48,885
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant